WASHINGTON – Congressman Spencer Bachus (R-Vestavia Hills) today said "basic" security steps can be taken to protect private personal information at the Veterans Administration (VA) and other federal agencies.

Bachus attended a congressional hearing that focused heavily on a data breach discovered at the VA Medical Center in Birmingham on January 23. A missing computer hard drive has potentially put the personal information of 535,000 veterans and 1.3 million physicians and health providers at risk.

"Encryption is a pretty elementary step. It should be standard operating procedure," Bachus told VA Deputy Secretary Gordon Mansfield during a hearing held by the House Veterans Affairs Committee.

While the VA has encryption policies, Bachus said the agency has not provided regional facilities like the one in Birmingham with the software needed to comply. The investigation is continuing into the data breach, which involved Social Security numbers, Medicare billing codes, and other sensitive information.

Bachus expressed concern that identification codes included in the medical information could be used to conduct Medicare and Medicaid fraud. The information contained such details as physician names, credentials, education, billing licenses, and Medicare billing codes.

There have been past reports warning of data vulnerabilities at the VA, Bachus observed.

"These actions have been waiting to happen since 1997," Bachus said, noting that internal government audits have given the agency a failing grade for data protection for the past five years.

Bachus, the ranking member on the House Financial Services Committee, has asked his panel to join in the investigation of data security concerns at government agencies.

###